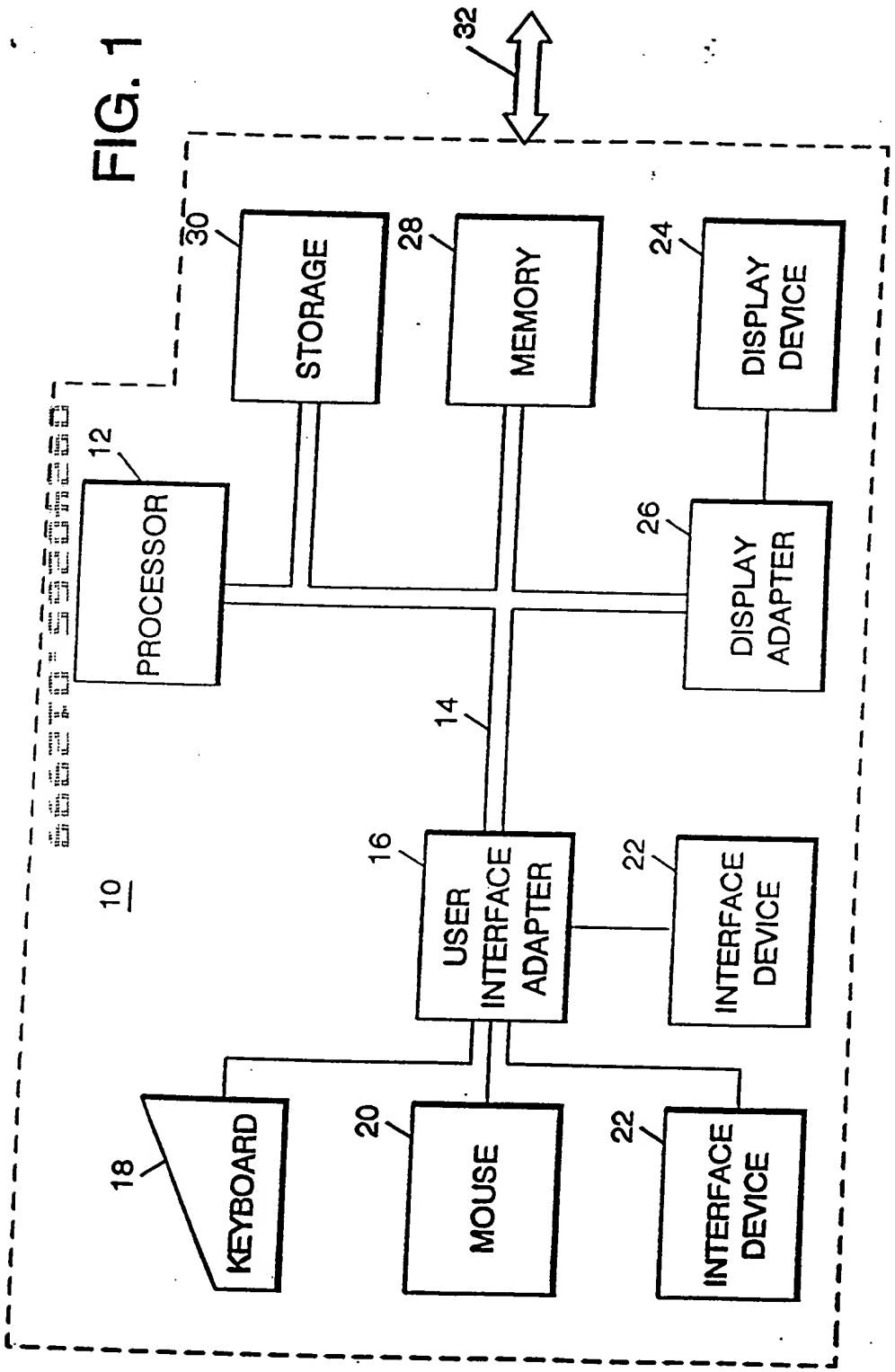
FIG. 1


32
30
STORAGE
28
MEMORY
24
DISPLAY DEVICE
12
PROCESSOR
26
DISPLAY ADAPTER
14
16
USER INTERFACE ADAPTER
22
INTERFACE DEVICE
10
18
KEYBOARD
20
MOUSE
22
INTERFACE DEVICE

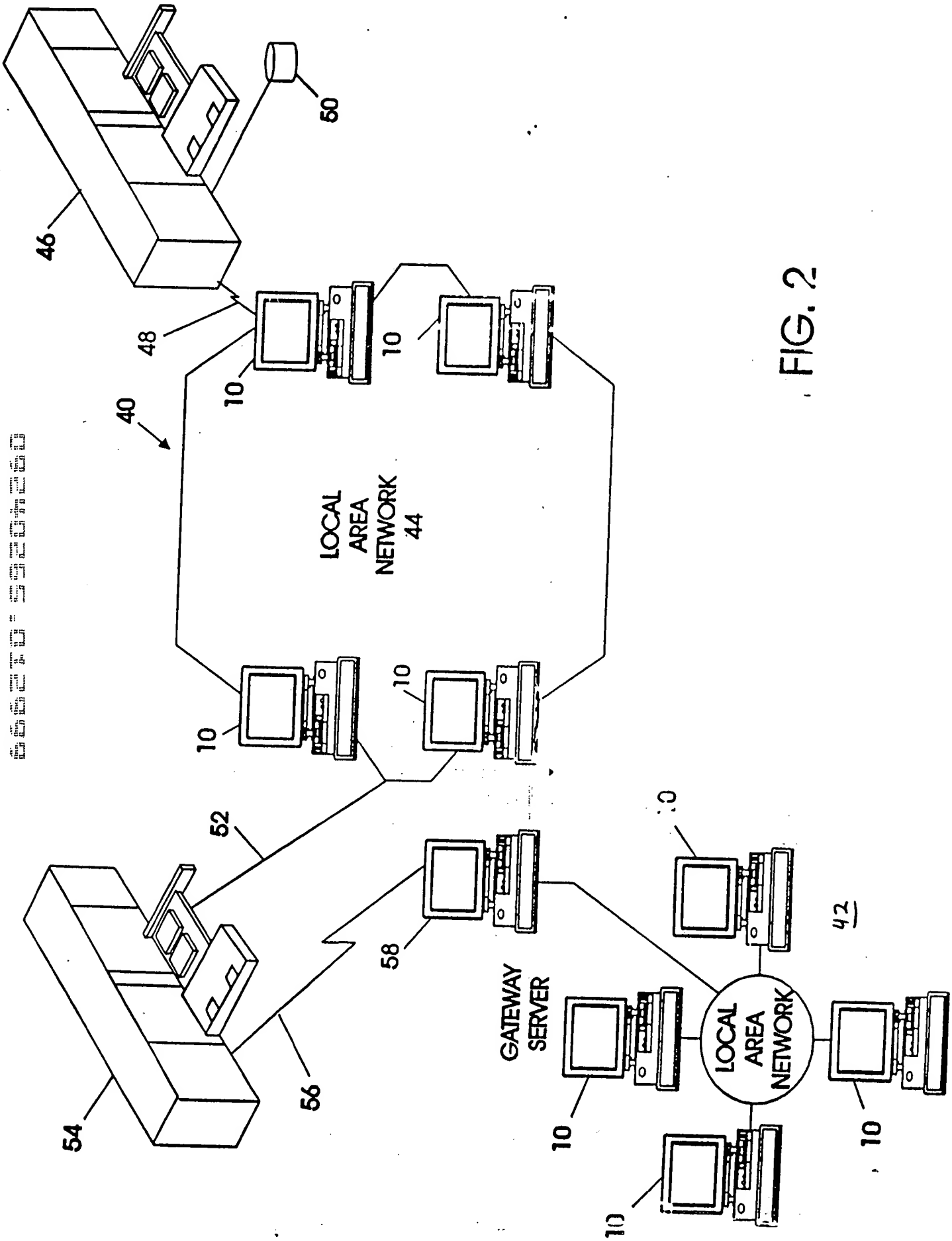

46
50
48
10
10
40
LOCAL AREA NETWORK 44
10
10
52
58
54
56
GATEWAY SERVER
LOCAL AREA NETWORK
42
10
10
10

FIG. 2

FIGURE 3

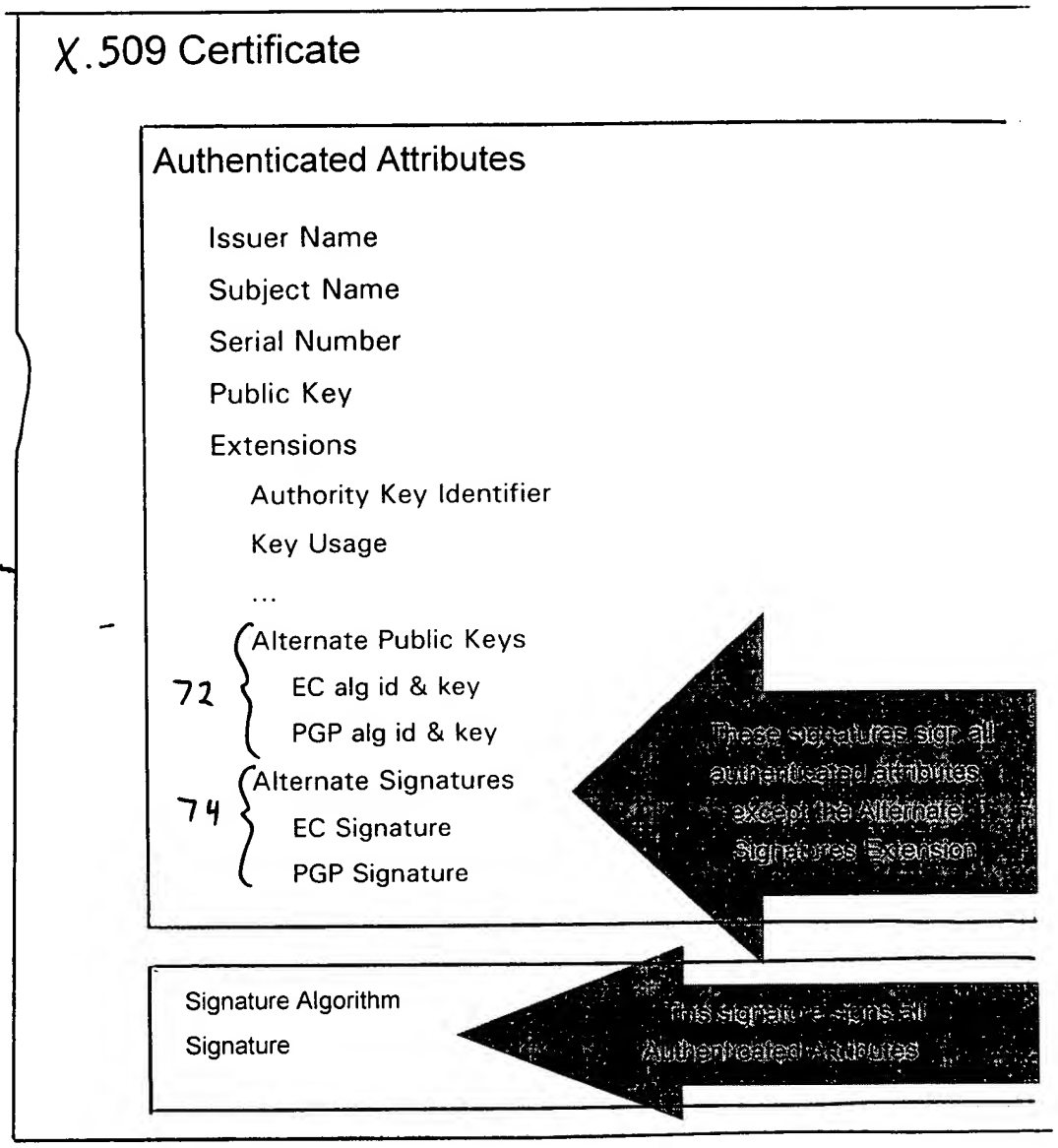
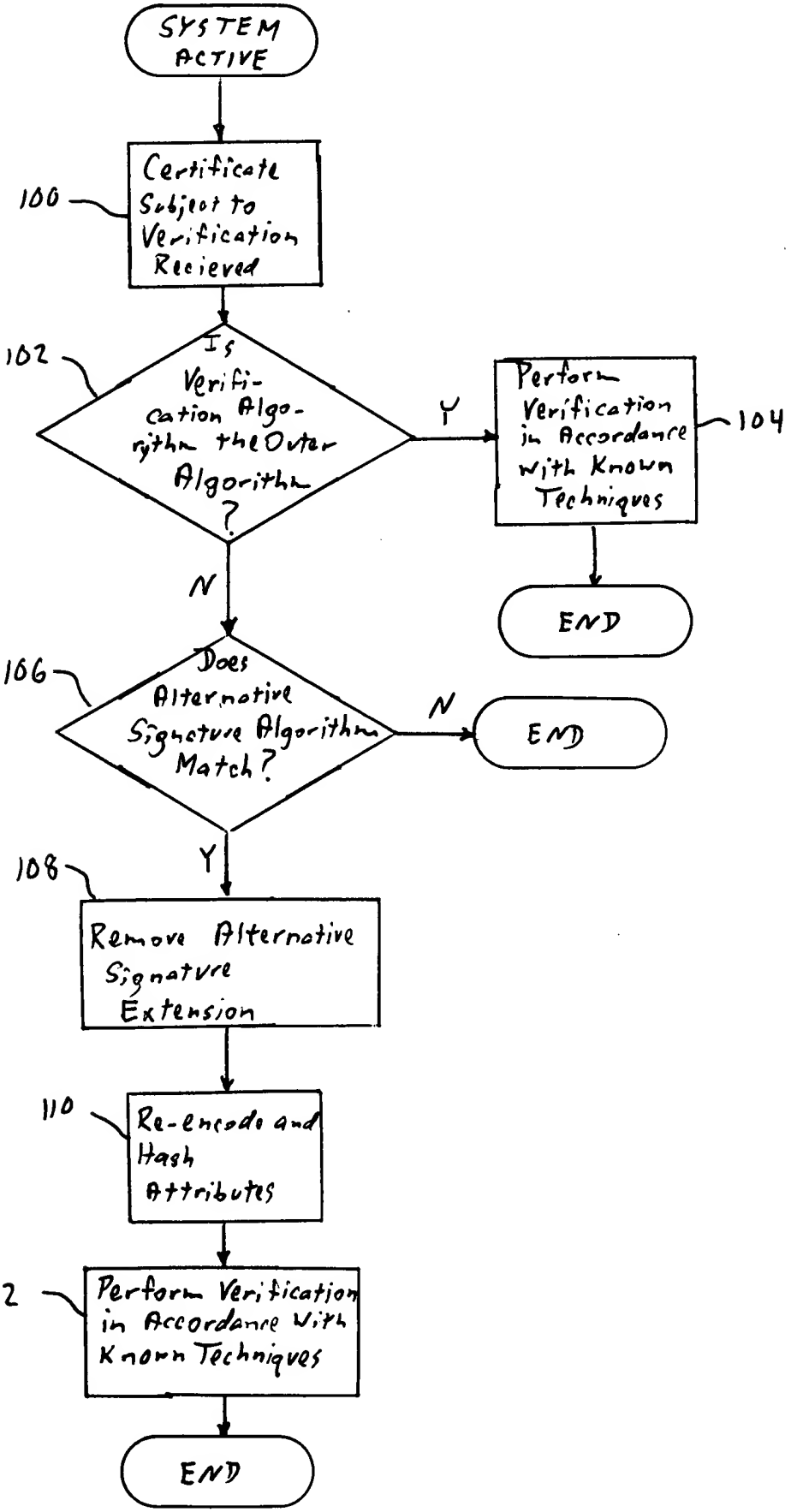

X.509 Certificate
Authenticated Attributes
Issuer Name
Subject Name
Serial Number
Public Key
Extensions
Authority Key Identifier
Key Usage
...
Alternate Public Keys
EC alg id & key
PGP alg id & key
Alternate Signatures
EC Signature
PGP Signature
These signatures sign all authenticated attributes except the Alternate Signatures Extension
Signature Algorithm
Signature
This signature signs all Authenticated Attributes
70
72
74

FIGURE 4


SYSTEM ACTIVE
Certificate Subject to Verification Recieved
100
Is Verification Algorithm the Outer Algorithm ?
102
Y
Perform Verification in Accordance with Known Techniques
104
END
N
Does Alternative Signature Algorithm Match?
106
N
END
Y
Remove Alternative Signature Extension
108
Re-encode and Hash Attributes
110
Perform Verification in Accordance With Known Techniques
112
END